Data Decommissioning

As part of the ongoing effort by the Enterprise Information Security Office to protect the confidentiality of state information, equipment sent to surplus property for disposal must have all data removed. Sounds simple, but not all data and file deletion methods remove the actual data.

There are a number of methods to delete data from a computer's hard drive (e.g., highlighting a file and pressing the Delete key, emptying a recycle bin or trash folder, or using system utilities to reformat the disk). However, these methods do not actually remove the data, they simply remove quick and easy access; the data remains on the hard drive. Readily available software tools can also be used to restore the data.
It is important that data be securely removed once devices are no longer in use.

To ensure all data is removed agency technical staffs are required to use drive wiping tools like DBAN or Wipe Drive. The enterprise information security office is using a new tool WipeDrive Pro from WhiteCanyon to audit computer hard drives at surplus property and verify that all information has been completely removed.

Employees responsible for sending computer equipment to surplus property must take the online Data Decommission Training so they understand the needed and method to successfully remove data from hard drives.